ABSTRACT OF THE INVENTION

[0045] A pseudo-random number generator (PRNG) with increased randomness. An iterative hash-based PRNG hashes in the output of a numerical sequencer, such as a counter or linear feedback shift register, in each hash stage. To improve the unpredictability of the numerical sequencer output, it may be paused for relatively unpredictable time periods. When the timing of the output of the numerical sequencer is unpredictable, elapsed time cannot be used to reliably predict what the output of the numerical sequencer will be with relation to the hash operation. The unpredictable time period may be related to when a request for a pseudo-random number is received.